**Amendments to the Specification**

On page 1, line 23 through page 2 line 4, please replace the existing paragraph with the following substitute paragraph:

By definition, a computer virus is executable program code that is self-replicating and almost universally unsanctioned. More precisely, computer viruses include any form of self-replicating computer code which can be stored, disseminated, and directly or indirectly executed. The earliest computer viruses infected boot sectors and files. Over time, computer viruses evolved into numerous forms and types, including cavity, cluster, companion, direct action, encrypting, multipartite, mutating, polymorphic, overwriting, self-garbling, and stealth viruses, such as described in "McAfee.com: Virus Glossary of Terms," ~~http://www.mcafee.com/anti-virus/virus_glossary.asp?,~~ Networks Associates Technology, Inc., Santa Clara, California (2000), the disclosure of which is incorporated by reference.

On page 5, line 29 through page 6 line 9, please replace the existing paragraph with the following substitute paragraph:

FIGURE 1 is a functional block diagram showing a distributed computing environment 10, including a system for identifying a macro virus family[[ 16]], using a macro virus definitions database, in accordance with the present invention. The networked computing environment 10 includes one or more servers 12 interconnected to one or more clients 13 over an internetwork 11, such as the Internet. Each server 12 provides client services, such as information retrieval and file serving. Alternatively, the clients could be interconnected with the server 12 using a direct connection, over a dial-up connection, via an intranetwork 14, by way of a gateway 15, or by a combination of the forgoing or with various other network configurations and topologies, as would be recognized by one skilled in the art.

On page 12, lines 10-17, please replace the existing paragraph with the following substitute paragraph:

First, the *.dat* file 42 (shown in FIGURE 4) is opened (block 137) and each line containing the source code text identified by the current token is found (block 138). The byte flag is set to the next byte flag *ReplFlags* (block 139) and iterative processing continues until all of the byte flags *ReplFlags* are complete (block 136). The search entry is then set to the next entry in the parse tree (block 141) and iterative processing continues through the parse tree until the parse tree is complete (block ~~133~~ 142). Finally, a report is output (block 143), after which the routine returns.

On page 78, lines 4-15, please replace the existing paragraph with the following substitute paragraph:

~~A system and method for identifying a macro virus family using a macro virus definitions database is described.~~ A macro virus definitions database is maintained and includes a set of indices and associated macro virus definition data files. One or more of the macro virus definition data files are referenced by the associated index. Each macro virus definition data file defines macro virus attributes for known macro viruses. The sets of the indices and the macro virus definition data files are organized according to macro virus families. One or more strings stored in a suspect file are compared to the macro virus attributes defined in the one or more macro virus definition data files for each macro virus family in the macro virus definitions database. The macro virus family to which the suspect file belongs is determined from the indices for each of the macro virus definition data files at least partially containing the suspect file.